The NAMA Show 2018
Meet with Convenience

MARCH 21-23
LAS VEGAS
CONVENTION CENTER

Understanding & Simplifying PCI Compliance

Chris Bucolo, ControlScan, Inc

Who is ControlScan?

- Trusted by more than 150 ISOs, acquirers and payment facilitators to deliver PCI compliance services to their merchant portfolios (over 1.1 million merchants in aggregate)
- Established PCI QSA and ASV company with a full range of assessment and testing services
- Managed Security Service Provider with value-added solutions that include:
  - PaySafe UTM Firewall
  - Log Monitoring and Management
  - Advanced Endpoint Security
- Award-winning, U.S.- housed security and compliance support services

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council™
APPROVED SCANNING VENDOR

Info Security Products Guide
2016
GLOBAL EXCELLENCE
GOLD
★★★★★

CISSP • CISM • CISA • CRISC • C|EH • GPEN • Network+ • Security+ • PCIP • OSCE

Today's Speaker

Chris Bucolo, PCIP
Director, Strategic Partnerships
& Market Strategy
ControlScan

Session Summary

- A brief look at where PCI started
  - 10 years and counting
- Key aspects of how PCI/Card brands address breach prevention today
  - The service provider factor: Remote Access/A few words about QIRs
  - The U.S. market: lots of magnetic stripe data-what about EMV?
  - What is the best approach to PCI & Security?
- Where it is heading moving forward
  - Mobile IOT explosion-its all about the software
  - PCI Council Small Merchant Task force efforts
- Top Takeaways List

Where It Started: The PCI Big Three

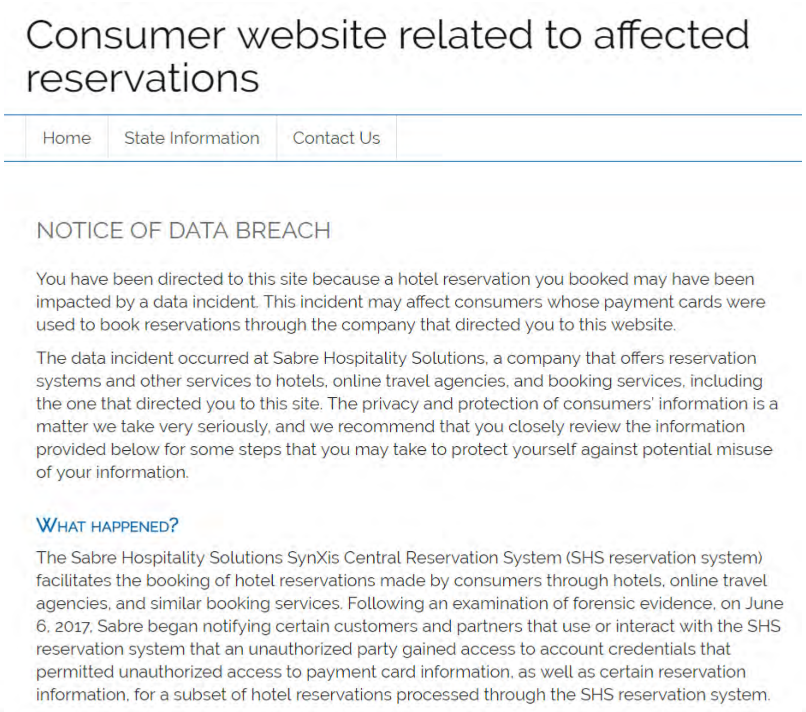
	PCI DSS	PA DSS	PTS (PED)
Overview	• The Payment Card Industry DSS (PCI DSS) is a data security standard managed by the PCI SSC • The standard was created to help organizations that accept card payments minimize exposure to a data breach	• The Payment Application DSS (PA-DSS) is a comprehensive set of requirements designed for payment application vendors • The program is designed to drive out prohibited data storage and foster a more secure payments system.	• The PCI PIN Security Requirements are primarily focused on device characteristics impacting the security of PIN Entry Devices (PED) • The PCI SSC manages the listing of approved PIN Transaction Security (PTS) Devices and the PCI PED security requirements
Applies To	• Any business that accepts or processes payment cards	• Software vendors that develop commercial payment applications that store, process or transmit cardholder data as part of authorization or settlement • Acquirers must ensure their merchants use only PA-DSS compliant applications (Visa) as applicable	• Vendors that manufacturer PIN-Entry Terminals • Merchants who accept PIN-based transactions (integrated terminal or standalone PIN pad) ***NOTE:** These devices may also be referred to as PTS Points-of-Interaction (POI)*

Where PCI Stands Today

- A mature standard- no more 3 yr. cycles
- Updates based on breach experiences
  - Service providers and remote access
  - Software explosion
  - Evolution of consumer driven buying experiences
    - EMV
    - High growth of transactions on consumer devices

Current U.S. Breach Experiences

The Broad Reach of Service Provider Breaches



Consumer website related to affected reservations

NOTICE OF DATA BREACH

You have been directed to this site because a hotel reservation you booked may have been impacted by a data incident. This incident may affect consumers whose payment cards were used to book reservations through the company that directed you to this website.

The data incident occurred at Sabre Hospitality Solutions, a company that offers reservation systems and other services to hotels, online travel agencies, and booking services, including the one that directed you to this site. The privacy and protection of consumers' information is a matter we take very seriously, and we recommend that you closely review the information provided below for some steps that you may take to protect yourself against potential misuse of your information.

WHAT HAPPENED?

The Sabre Hospitality Solutions SynXis Central Reservation System (SHS reservation system) facilitates the booking of hotel reservations made by consumers through hotels, online travel agencies, and similar booking services. Following an examination of forensic evidence, on June 6, 2017, Sabre began notifying certain customers and partners that use or interact with the SHS reservation system that an unauthorized party gained access to account credentials that permitted unauthorized access to payment card information, as well as certain reservation information, for a subset of hotel reservations processed through the SHS reservation system.

FOUR SEASONS
HOTELS AND RESORTS

Hard Rock
HOTEL

RED LION HOTELS
CORPORATION

KIMPTON®
HOTELS & RESTAURANTS

The Service Provider Factor

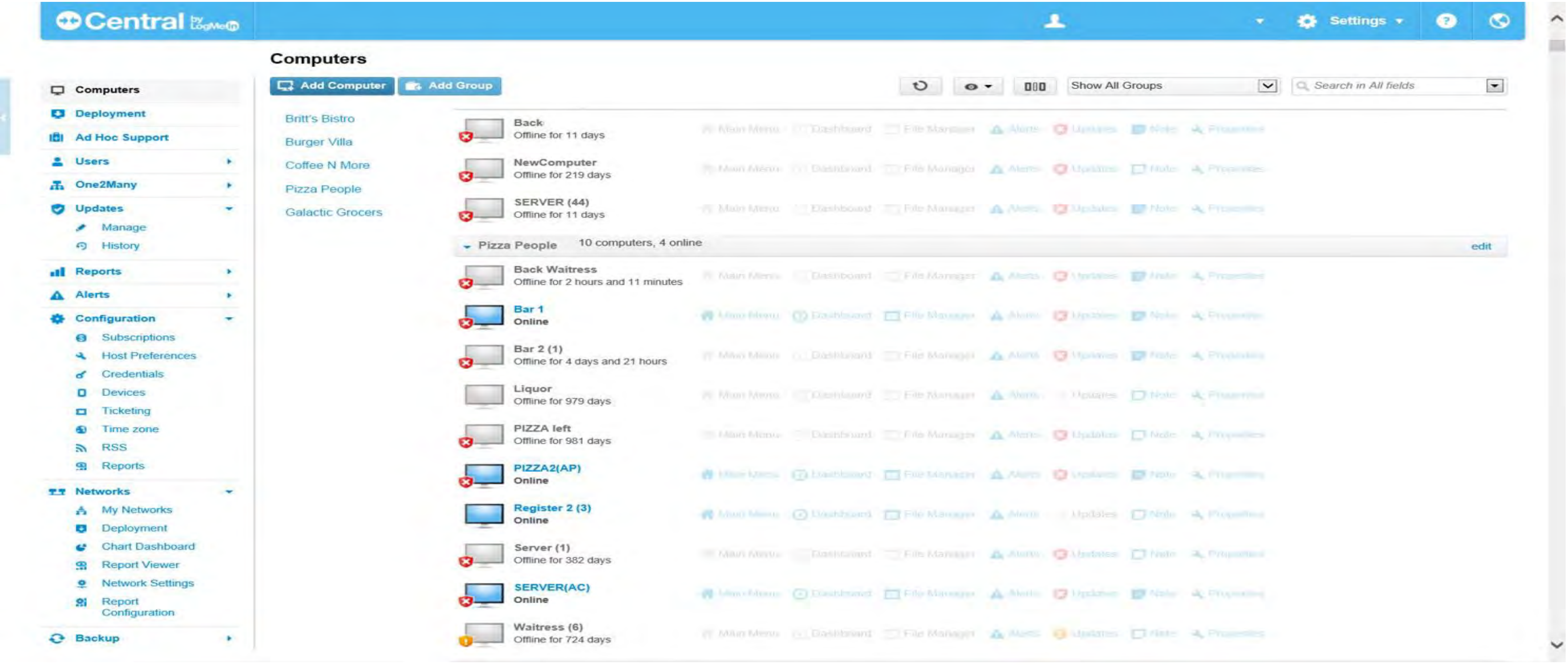
Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity.

→ **This includes providers of services that control or could impact security of cardholder data.**

→ Examples include managed service providers for managed firewalls, IDS and other services, as well as hosting providers and other entities.

Note: Any third party with remote access into a merchant’s cardholder data environment can impact security, and will be viewed as a service provider.

Remote Access Breach Formula



Computers

Back	Offline for 11 days
NewComputer	Offline for 219 days
SERVER (44)	Offline for 11 days

Pizza People 10 computers, 4 online

Back Waitress	Offline for 2 hours and 11 minutes
Bar 1	Online
Bar 2 (1)	Offline for 4 days and 21 hours
Liquor	Offline for 979 days
PIZZA left	Offline for 981 days
PIZZA2(AP)	Online
Register 2 (3)	Online
Server (1)	Offline for 382 days
SERVER(AC)	Online
Waitress (6)	Offline for 724 days

The PCI Council & Card Brands Response

PCI DSS Compliance

"If you are a merchant that accepts payment cards, you are required to be compliant with the ***Payment Card Industry Data Security Standard*** *(PCI DSS)."*

PCI Security Standards Council®

- ✓ Must achieve compliance annually
- ✓ Must validate compliance (effective Jan. 31, 2017)
- ✓ Must use a QIR certified technician to install POS systems (effective Jan. 31, 2017)

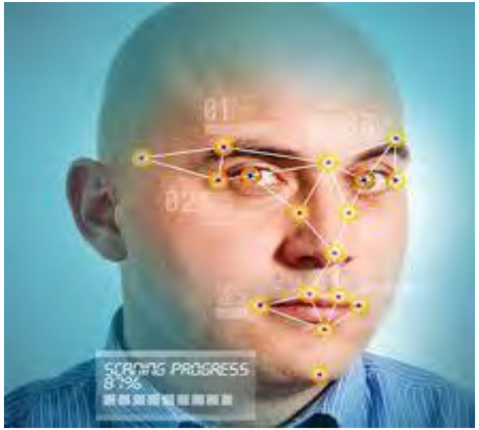
Source: www.pcisecuritystandards.org

PCI SAQ v3.2: New Service Providers Reqs. Kick-in

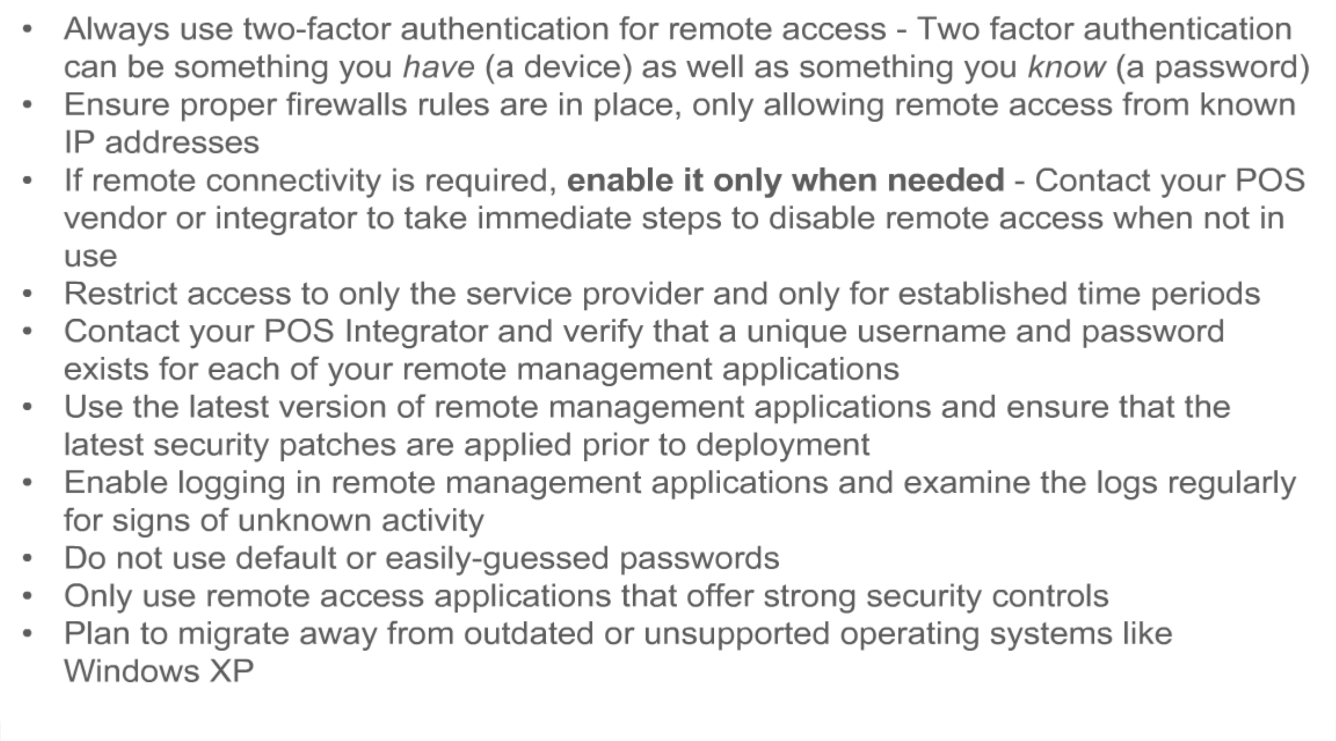
- **As of February 1, 2018**:
  - **6.4.6** Material changes require that PCI DSS requirements be applied to all new or changed systems and networks, with updated documentation
  - **8.3.1 Utilize multi-factor authentication for non-console administrative access to CDE, locally and remote** (this has already been in place for remote access)
  - **10.8** A process must be in place for detecting and reporting a failure of critical systems, along with an action plan for responding
  - **11.3.4.1 Penetration tests for network segmentation must now be completed every 6 months by a qualified internal or external resource**
  - **12.4.1** Executive management must establish accountability for maintaining PCI DSS compliance and define the charter
  - **12.11** Quarterly reviews must be performed and documented to ensure that personnel are following security policies and procedures

What is Multi-Factor Authentication?

- 3 factor covers:
  - What you know (Password, PIN)
  - Something you Have (card, phone)
  - Something you are (unique to you-cannot be changed: Biometrics: Face, fingers, heart rate, movement, etc.)



How to Mitigate The Remote Access Risk



- Always use two-factor authentication for remote access - Two factor authentication can be something you *have* (a device) as well as something you *know* (a password)
- Ensure proper firewalls rules are in place, only allowing remote access from known IP addresses
- If remote connectivity is required, **enable it only when needed** - Contact your POS vendor or integrator to take immediate steps to disable remote access when not in use
- Restrict access to only the service provider and only for established time periods
- Contact your POS Integrator and verify that a unique username and password exists for each of your remote management applications
- Use the latest version of remote management applications and ensure that the latest security patches are applied prior to deployment
- Enable logging in remote management applications and examine the logs regularly for signs of unknown activity
- Do not use default or easily-guessed passwords
- Only use remote access applications that offer strong security controls
- Plan to migrate away from outdated or unsupported operating systems like Windows XP

Penetration Testing Vs. Scanning

- Due to breach forensics more SAQs (Self-Assessment Questionnaires) require scanning & Penetration testing.
- Increased requirements for service providers

Medical Analogy: MRI Vs. Exploratory surgery

"It's kind of an exploratory surgery to see what can be done and if I can find my laser pen."

© Jonny Hawkins 2015

QIRs-Qualified Integrators & Resellers

“Numerous breach investigations have shown that **incorrect installation and/or maintenance of payment applications creates opportunities for merchant networks to be compromised.**

“Integrators and resellers play a key role in the payments ecosystem, as merchants depend on these service providers to install, configure, and/or maintain their validated applications.

“This program outlines guiding principles and procedures for the **secure installation and maintenance of validated payment applications in a manner that supports PCI DSS compliance.”**

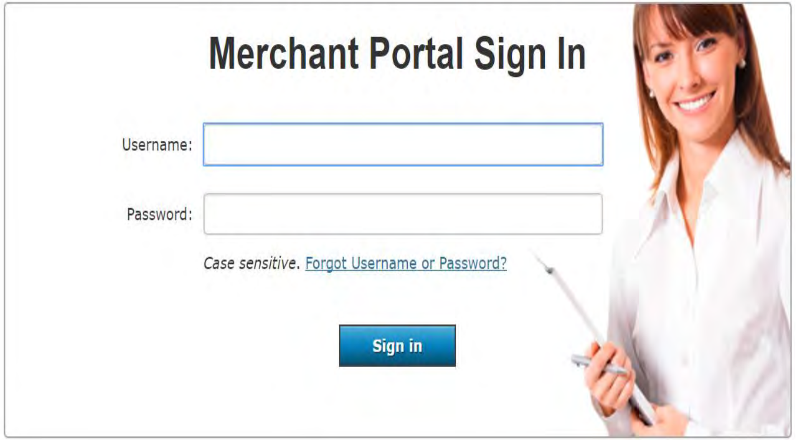
→ https://www.pcisecuritystandards.org/program_training_and_qualification/qualified_integrator_and_reseller_certification

Right for you if…

You’re an integrator or reseller that **sells, installs, and/or services PA-DSS validated payment applications on behalf of software vendors or others.**

What is The Best Approach?

Enroll in a PCI program- Complete Online



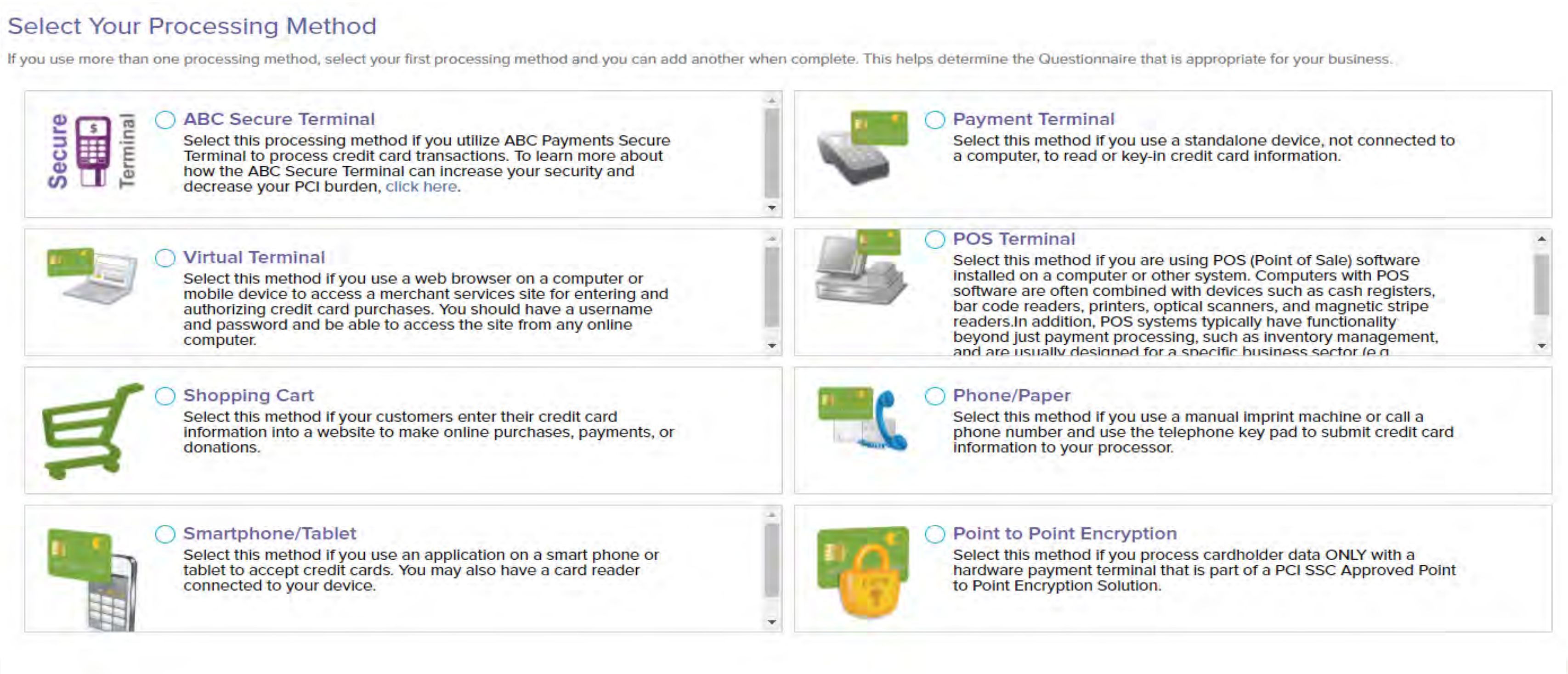
Merchant Portal Sign In

Username:

Password:

Case sensitive. Forgot Username or Password?

Get Pointed to The Correct SAQ!!



Select Your Processing Method

If you use more than one processing method, select your first processing method and you can add another when complete. This helps determine the Questionnaire that is appropriate for your business.

○ **ABC Secure Terminal**
Select this processing method if you utilize ABC Payments Secure Terminal to process credit card transactions. To learn more about how the ABC Secure Terminal can increase your security and decrease your PCI burden, click here.

○ **Payment Terminal**
Select this method if you use a standalone device, not connected to a computer, to read or key-in credit card information.

○ **Virtual Terminal**
Select this method if you use a web browser on a computer or mobile device to access a merchant services site for entering and authorizing credit card purchases. You should have a username and password and be able to access the site from any online computer.

○ **POS Terminal**
Select this method if you are using POS (Point of Sale) software installed on a computer or other system. Computers with POS software are often combined with devices such as cash registers, bar code readers, printers, optical scanners, and magnetic stripe readers.In addition, POS systems typically have functionality beyond just payment processing, such as inventory management, and are usually designed for a specific business sector (e.g.

○ **Shopping Cart**
Select this method if your customers enter their credit card information into a website to make online purchases, payments, or donations.

○ **Phone/Paper**
Select this method if you use a manual imprint machine or call a phone number and use the telephone key pad to submit credit card information to your processor.

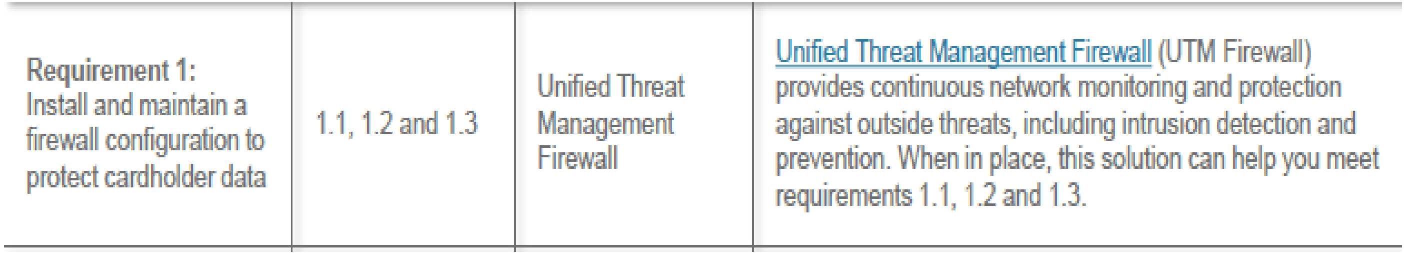
○ **Smartphone/Tablet**
Select this method if you use an application on a smart phone or tablet to accept credit cards. You may also have a card reader connected to your device.

○ **Point to Point Encryption**
Select this method if you process cardholder data ONLY with a hardware payment terminal that is part of a PCI SSC Approved Point to Point Encryption Solution.

Find out Which Security Offerings Match-up

	Firewall UTM	Logging	FIM	Anti-Virus	Sec Aware Training	Internal Scanning	External Scanning
SAQ A							
SAQ A - EP	✓	✓	✓	✓	✓		✓
SAQ B					✓		
SAQ B - IP	✓				✓		
SAQ C	✓	✓	✓	✓	✓	✓	✓
SAQ C - VT	✓			✓	✓		
SAQ D - M	✓	✓	✓	✓	✓	✓	✓
SAQ D - SP	✓	✓	✓	✓	✓	✓	✓
SAQ P2PE					✓		

Merchant Benefits – Ease of PCI Compliance



Requirement 1: Install and maintain a firewall configuration to protect cardholder data	1.1, 1.2 and 1.3	Unified Threat Management Firewall	Unified Threat Management Firewall (UTM Firewall) provides continuous network monitoring and protection against outside threats, including intrusion detection and prevention. When in place, this solution can help you meet requirements 1.1, 1.2 and 1.3.

- By utilizing UTM firewall , MSSP assumes responsibility for the Requirements 1.1, 1.2, and 1.3 and the PCI-DSS 12 steps for compliance.
- Additionally and when implemented in conjunction with the PCI 123 SAQ solution, assumed sections of compliance are automatically pre-populated to decrease the amount of effort and time to self attest.

Tampering and Skimming

- PCI DSS requirement 9 addresses physical security controls
- In the fuel retail environment, physical security pertains to the controls necessary to protect card data in its many forms – including manual imprints and other printed forms of cardholder data that may only occur during network outages.
- The unique environment in the petroleum world necessitates that attention be paid to both <u>inside</u> and <u>outside</u> assets, especially those involving payment devices. There is evidence that skimming and tampering attacks have gotten more sophisticated and, often have become more successful. (source: Verizon DBIR-2016)

Work on The Human Element

- Passwords
- Remote access-human intervention is best. Caveat- if done right-sword cuts both ways
- Social engineering-Phishing is huge!!
- Be a skeptic even if people get ruffled sometimes-not customers of course ☺

Where is PCI Heading?

Wasn't EMV Supposed to Fix All This?

- 50%-55% merchant outlets penetration
- Card present card fraud reducer for sure
- But magnetic stripe data alive and well on the dark web-RAM scraping
- EMV alone vs. EMV plus P2PE/E2EE!!!

Things To Look For

- Streamlined QIR program-March 2018
  - Remote access/Passwords/Software updates
- More focus on software/equipment security
- More emphasis on ecommerce breach risk
- More emphasis on technology answers:P2PE
- New alternative to SAQs from Small merchant task force

Call To Action in The Marketplace

Merchant: How can we streamline and simplify PCI?

Card Processor: How do you achieve strong security at the same time?

If done well: it is a win-win.

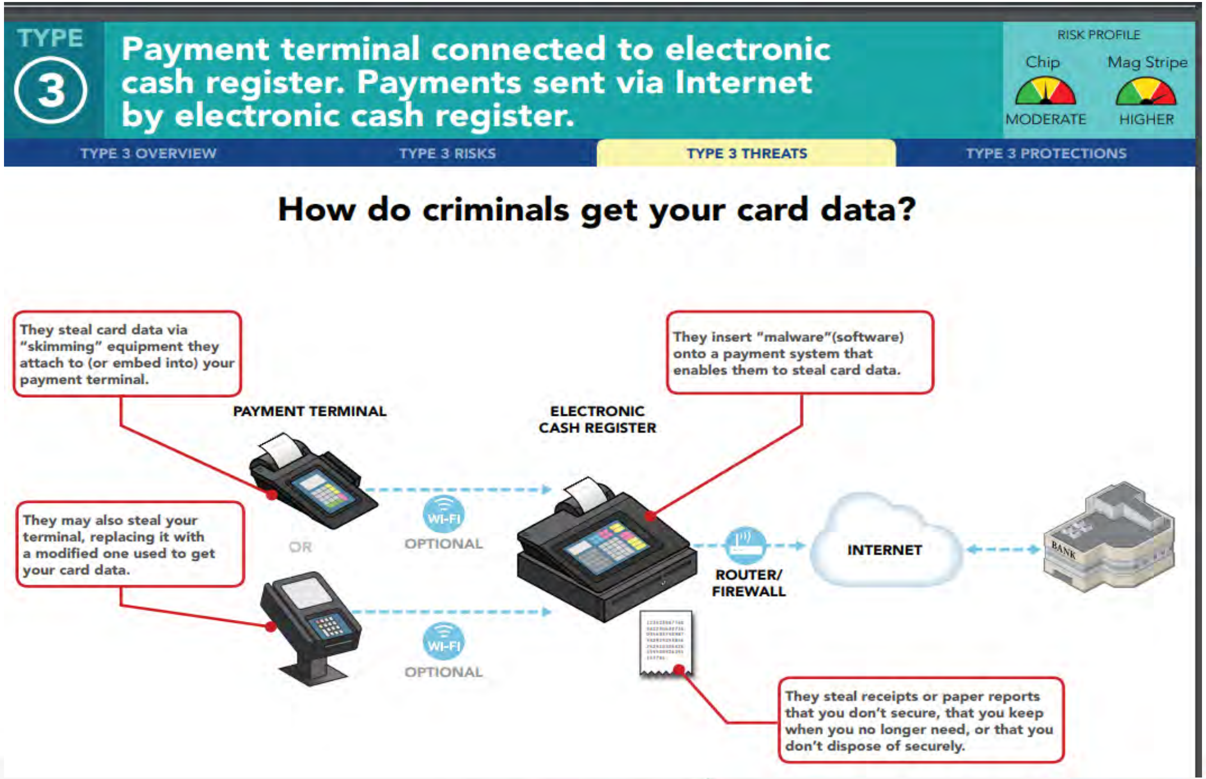
- Our View: Authentic Compliance + Strong Security = Winning Risk management Strategy
- The number 1 need is to find a few "trusted advisors."

PCI Small Merchant Task Force

- Building on past work to create simpler ways of understanding security concepts
- Initial release: good work but not married to SAQ process
- First efforts to truly look at risk of how you process-and suggested ways to mitigate it
- **Current effort will release SAQ alternative-"Data Security Essentials" for low to medium risk scenarios-April 2018**
  - **Consolidation of concepts into fewer questions**
  - **Every effort made to simplify-with more explanation as back-up**
  - **Risk focus**

PCI Small Merchant Task Force

Higher Risk Scenario



TYPE 3

Payment terminal connected to electronic cash register. Payments sent via Internet by electronic cash register.

RISK PROFILE

Chip: MODERATE

Mag Stripe: HIGHER

TYPE 3 OVERVIEW | TYPE 3 RISKS | TYPE 3 THREATS | TYPE 3 PROTECTIONS

How do criminals get your card data?

They steal card data via "skimming" equipment they attach to (or embed into) your payment terminal.

They may also steal your terminal, replacing it with a modified one used to get your card data.

They insert "malware"(software) onto a payment system that enables them to steal card data.

They steal receipts or paper reports that you don't secure, that you keep when you no longer need, or that you don't dispose of securely.

Top Takeaways

- PCI is here to stay!- 10 years and counting
- For small businesses PCI is the basis for security knowledge and action plans
- Complying with PCI is typically not expensive for small businesses
    - The alternatives usually are expensive-breach related costs/brand damage

Typical vulnerabilities:

- Remote Access*
- Password Strength*
- Software updating/patching*

*New QIR focus.

- Firewalls with established rules to restrict traffic and manage risk
- Physical Fraud-skimmers, PIN Pad overlays, etc.
- The human element!!

Q
&
A

The NAMA Show 2018
Meet with Convenience

MARCH 21-23
LAS VEGAS
CONVENTION CENTER

Contact Info:

cbucolo@controlscan.com | P: 678-279-2646
C: 610-914-9555

Connect with @ControlScan: in t f her g+ , P You Tube & Possibilities Meet